1c Reg

21 November 1975

MEMORANDUM FOR: Deputy to the DCI for the Intelligence Community

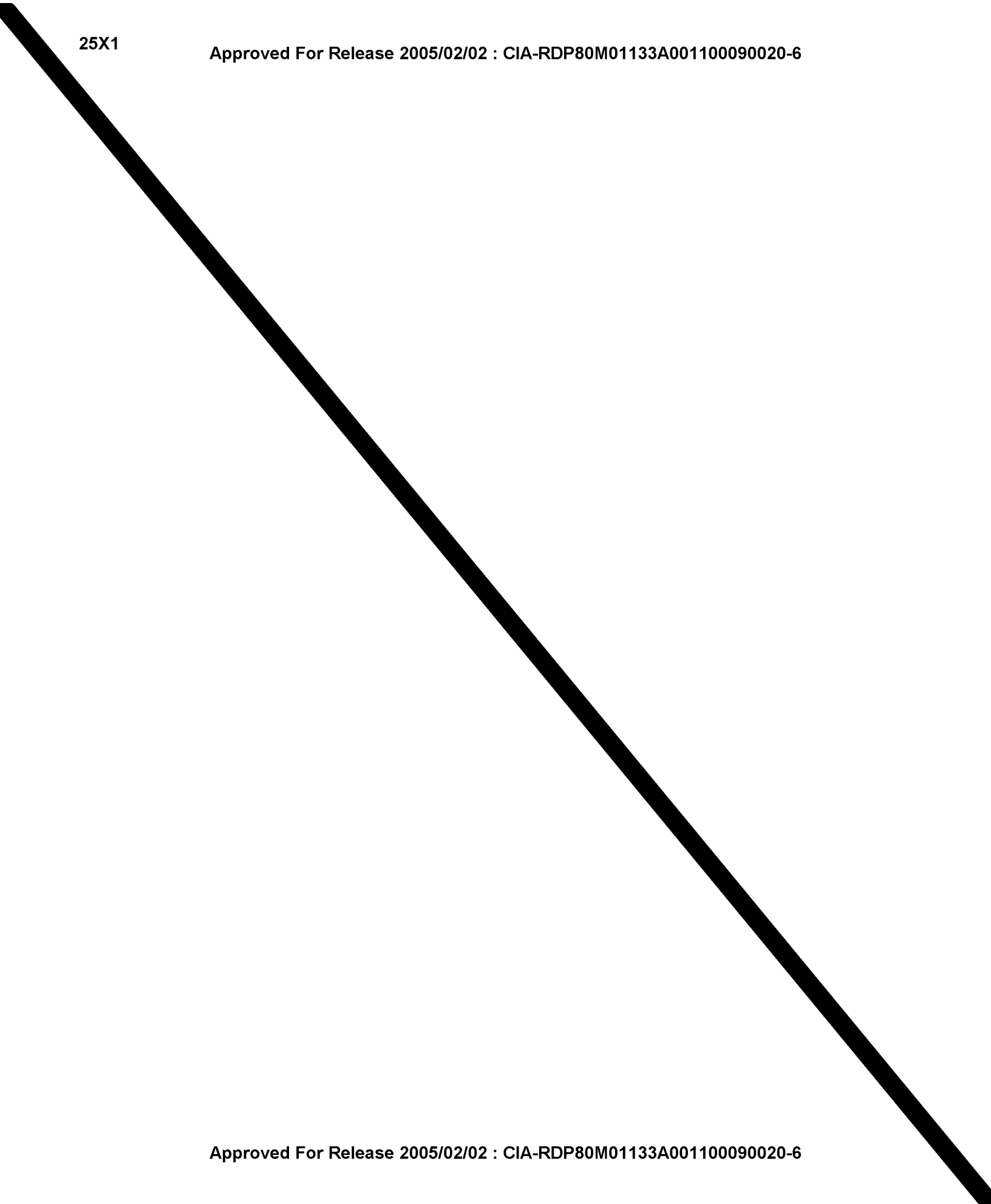
SUBJECT: The Secrecy Problem

1. The attached paper on the Secrecy Problem represents the best I could do in the extremely short time I was given. It is based on reading hundreds of pages both historical and current, and on many conversations with interested and knowledgeable parties--though not nearly so many as the problem requires. It does not respond to all the matters raised by Hank Knoche when he asked me to write the paper, but it does try to distill some perceptions and attitudes that come from thirty years of work within the many security systems of the Community--not as an expert on those systems' complexities but as one of the thousands whose work they have governed. I hope my effort to read back into the problem after several years away from it has not left glaring misstatements of fact.

25X1 [redacted]

25X1 [redacted]

Attachment:
As stated



Approved For Release 2005/02/02 : CIA-RDP80M01133A001100090020-6

21 November 1975

1. So much careful study has been lavished upon the Intelligence Community's security problems that a brief new study now can highlight only three aspects, and draw attention to other recent writings which offer prospects of important improvements. These prospects will be enhanced if serious attention is given to these three aspects:

a. The situation requires more urgent and drastic action than has been generally recognized.

b. The present security system is so complex as to be unworkable. Its provisions are self-defeating both in the protection of sensitive materials and in assuring sufficient access to those materials by those who need them. It is a delusion to suppose that proper discipline can be inculcated in the whole Intelligence Community and among the outside users of its products unless the system is drastically simplified and made intelligible to all who must be governed by it.

c. It must be recognized that the security system's complexity comes from the perpetuation of principles and practices that were suitable for a simpler age but are now anachronisms. One reason for this is the changing position of intelligence within American society, but an even more important cause of the problem is the steady growth in quantity and complexity of what needs protecting.

2. The problems of compartmentation, classification, dissemination, tasking and requirements, and both optimum and maximum use of the materials the Intelligence Community collects and analyzes, are all closely related with one another. Each has been repeatedly and conscientiously studied over many years by various elements of the Community, sometimes with good results, but for the most part the problems of security- vs.-optimum-production have been studied in isolation from each other. Ever since World War II the various protective systems have become more complex, more numerous, and more difficult to administer with total fidelity to the thousands of detailed provisions in all the laws, executive orders, directives, regulations, manuals, and other guidelines both written and unwritten. No individual in the system, however devoted to the principles of security, can hope to know, understand, and remember all the rules; if he tries to master and keep up to date on them (as most do not), he has no time for anything else.

3. It is time to find a new approach. The Community should study the security system as a whole, not one or another of its component parts in isolation. All its parts affect one another, and if they are allowed to go on growing haphazardly as they have done for the most part for thirty years, the system is bound to become more and more self-deluding and self-defeating. When it becomes clear that the system is not working, least of all in the crucial matter of preventing deliberate leaks, the action required is not just adding new rules to a collection already hopelessly complex. What we need is a fundamental reform of the system, including sufficient simplification for each member of the Community to understand and carry out his proper share in the security function. Even that will not prevent the high-level leaks which our political and governmental traditions encourage, but it will increase the chances that proper indoctrination will lead to proper discipline.

4. In the years during which nearly all intelligence problems revolved around the military threat to our survival, it was inevitable that procedures which had sufficed for military intelligence units would be adapted with little change for national intelligence of the whole Community. Rules and definitions for classification of documents, for example, grew out of World War II's Army Regulation 380-5, and two generations of intelligence officers were taught that these familiar principles were immutable. They are still embedded in E. O. 11652 of 8 March 1972, but remain nearly as vague and subject to arbitrary

individual or institutional judgment as ever. Top Secret information is that which "requires the highest degree of protection" to prevent "exceptionally grave damage"--but it is now many years since the codeword system added higher and higher degrees of protection beyond Top Secret. In any case intelligent people will forever disagree over whether disclosure of a specific item of information would cause "exceptionally grave damage" as distinct from "serious damage." E. O. 11652 tries to define its terms by giving examples, but these also collapse under the vagueness of words like "vital" and "sensitive" (i.e., Top Secret) and "significant" (Secret) and the undefined border between them. Since everyone responsible for intelligence operations regards them all as "sensitive," Top Secret comes to mean whatever any authorized person chooses it to mean. The whole concept dates from an era which supposed that any disclosure by any means would cause such-and-such a degree of damage, as if that were measurable. We know now that the extent of damage depends also on how a disclosure is made, how much is disclosed, in what context, and especially when and by whom. In short, E. O. 11652 is not a workable basis for solving the security problem.

STAT

5. The rules for COMINT grew out of wartime practices, [redacted] which worked fairly well when the quantity of material to be protected was small enough to handle with extreme care. The proliferation of material, and of types of signals, and the decay of compartmentation by the ever-growing number of SI clearances, have caused the SIGINT community to insist more and more on protection of its material at the expense of its optimum use. In particular the enormous growth of SIGINT material collected by advanced technology (now more than half the total) has led to what many users and even some producers regard as unrealistic and unnecessary restriction of access.

STAT

6. This history was repeated in the gradual development of technical collection systems. They became steadily larger and more complex, and practices which were devised to protect their operations and products had to contend with growing conflicts among competing interests. The need for one kind of protection within the industrial community was not entirely compatible with the need for another inside the Intelligence Community. There was a conflict between security policy as executed by the NRP and public policy as represented by NASA; a variant of this problem lingers in the current debate over "the fact of" satellite reconnaissance. It illustrates the fact that intelligence information, along with sources and methods, needs different degrees of protection at

various levels of collection, production, dissemination, and end use. These needs change from subject to subject and from year to year. It is surely time for the Community to agree, for example, that analysts need considerably more access to primary data than end users. The work of both suffers when either too narrow compartmentation or drastic sanitization is introduced too early into the intelligence production process.

7. The complexities of classification, dissemination, and compartmentation have been better understood year by year, but what has not received sufficient attention as a primary cause of these complexities is the problem of sheer size. Our multifarious procedures were developed step by step when it was supposed that each new category of classification and compartmentation could be kept small enough to handle. But each new system was generally added to all the old ones, and each accretion made the system less workable, no matter how sensible were the rules devised for each accretion by itself. Meanwhile the quantity of information kept on growing, sometimes in quantum jumps, and was handled steadily less effectively under rules that had sufficed when all agreed that the quantity of our information was far too little for safety. The pressures to collect more and more naturally produced more and more, and the most crucial information was gradually overwhelmed by the less crucial and even the trivial. In my view this problem of size is both the principal cause of the erosion of security systems and the principal problem to be solved in devising a new system that will work. Reforms of the security system itself in all its aspects of classification, compartmentation, dissemination, use of the raw material and the end product, etc., will be merely palliative and cosmetic until the U. S. Government, as both producer and consumer of national intelligence, can reduce its requirements to a workable size.

8. By any reckoning the Government needs more good intelligence than ever before, and the need will continue to grow. How much it needs, and of what, is of course too vast a subject to be treated in a brief essay, but one aspect of it bears on our present subject: workload. If policy-makers received reasonably accurate answers to such questions as the following, they would insist on a thorough overhaul of the systems and practices designed to protect the Government's secrets:

a. How many million classified documents are already in the intelligence system? How many million photographs? How many million recordings? How fast are they accumulating? What are the projections for the next five years? Ten years?

b. What is the manpower situation, present and prospective? In particular, what is the relationship between numbers of clearances and the workload of the total intelligence population, and how does this vary over the years? What real compartmentation is possible when by our latest figures (July 1973) a minimum of 136,000 people hold SI clearances alone? (Why must we rely on figures more than two years old, and known to be far from complete? One expert estimates that the total number of SI clearances is at least 175,000. The security system cannot even guess at the number who have held SI clearances in the past, but experts have estimated upwards of a million.) We know roughly a minimum total number of clearances in all the compartmented systems--nearly 300,000--but there are no figures for the total number of people who hold clearances, since the separate systems are not integrated sufficiently, and we know that thousands of people hold more than one clearance. It is unlikely that many of them could give an accurate account of all the clearances they hold and what they stand for. The Chairman of the Intelligence Research and Development Council, for example, points out that "The overall security level established for the operation of the

[redacted] 25X1

least 195 clearances for the twelve members of the Council and its executive director, but this is not enough. The Chairman also points out: "Compartmentation and, in many cases, over-classification continue to serve as hindrances to effective cross-program communications among intelligence R&D planners. The Council serves to bridge this gap at the policy level; the R&D Planning Document improves communication among those planning staffs personnel who possess a wide array of commonly held access clearances. However, there continues to be a need to grant additional clearances within individual organizations to enhance cross-program communications." This example could undoubtedly be multiplied many times over within the Community.

c. What is the foreseeable impact of regulations already on the books with respect to the total holdings of the Intelligence Community? In particular, what is the impact on all our other functions of the workload entailed in all the provisions of E. O. 11652 for mandatory review, downgrading, declassification, etc., and the workload imposed by the Freedom of Information Act at all levels from executive, for policy determination on a wide variety of categories, down to the teams which have to search out and review all the materials requested? And what impact must we foresee from prospective changes in Congressional oversight and determination of what materials Congressional committees choose to publish? In addition to the grave security problems created by developments in these and related fields, we must expect a drastic increase in sheer unproductive workload of handling materials under E. O. 11652, FOIA, and Congressional attention to the Community. None of these problems will go away when the current investigations are concluded; they and increased attention from the media and a small vocal segment of the public are with us from now on.

d. What can we learn from the problem of backlogs, with which the Community has been wrestling for years, and which are bound to increase with such developments as the advent of near-real-time readout reporting?

e. How much does the whole security system cost, and what would an alternative, simplified system cost?

9. Despite the staggering size of the problem, it has been attacked repeatedly, creatively, and usefully over the past several years. This present brief study can hardly hope to accomplish more than to draw useful attention to three much more thorough studies. I believe they embody both the general principles and the specific proposals which would go a long way towards bringing the security systems under workable control. In my view these studies demonstrate that it is desirable and possible to:

a. Create a single system of Foreign Intelligence Information, distinct from national security information as defined in E. O. 11652, and bring it (with appropriate

recognition of different levels of sensitivity) under the DCI's responsibility for protection of intelligence sources and methods.

b. Define precisely what is covered by the term "intelligence sources and methods," and publish a list of its aspects (updated from time to time as appropriate) for the guidance of those authorized to create or use Foreign Intelligence Information.

c. Formulate and establish one manageable and practical system for the discrete compartmentation of intelligence and intelligence information related to designated sensitive sources and methods.

d. Preserve within this single system those aspects of the old systems which remain necessary: e.g., secrecy agreements, uniform criteria for access, and determination at the appropriate organizational level of an individual's need for some specific access.

e. Simplify other aspects, such as document markings, so that every holder of a clearance will know precisely what is required for secure handling and use of material, rather than continue his present bafflement or apathy when confronted with a bewildering variety of codewords.

f. Continue the decompartmentation successfully begun with large categories of TK material and now urged for other categories of sensitive intelligence by [redacted] 25X1 in his memorandum of 17 November 1975 to the DCI. 25X1

g. Shift the Community's emphasis somewhat from maximum protection of materials which no longer need it toward optimum use by the producers of intelligence, under guidelines which reflect what many of us see as a growing consensus within the Community.

10. The three studies referred to above are:

a. CIA Staff Review of [redacted] Compartmentation Systems of February 1972 (Top Secret [redacted] This exhaustive study, conducted by senior representatives of the Deputy Directors and the General Counsel under the chairmanship of [redacted] did bring about some useful small changes, such as the elimination of the barriers inside the Headquarters Building of CIA. For the most part, however, it did not receive the attention and action I believe it deserved. Some of its readers thought it too detailed and specific, others did not agree that any important action was needed; in some respects it has been overtaken by events, in others it needs restudy in the Community context. But in its main outlines (particularly in the argument for revising all compartmentation systems into a single system) it deserves renewed attention by the DCI and his deputies, and its draft of a new DCID entitled "Intelligence Security Compartmentation Guidance" deserves special study by the USIB subcommittee working on that problem.

b. "Security and Compartmentation of Foreign Intelligence Information," an unpublished paper by [redacted] Its latest (fourth) draft is dated 12 September 1975, when he was still executive secretary of the Security Committee of USIB. Some editing is still required, but it could be forwarded to the DCI within a few days. It is much shorter and less detailed than the [redacted] study, but marches along the same line of argument, and is based on [redacted] long years of experience with the problem, years during which he became one of the Community's most knowledgeable experts on the matters he discusses. Its proposals have not won universal acceptance among those who have already read it, and it does not pretend to solve all the problems, but the growing sense of urgency in the Community should accord it most serious attention. For myself, I find it fully persuasive.

c. "Aspects of Intelligence Sources and Methods that must be Protected from Unauthorized Disclosure," a draft currently in preparation for forwarding to the DCI by the General Counsel. It represents many months of work by a group under the leadership of [redacted] of the OGC, and has been widely coordinated within the Agency. If the DCI accepts this or a similar detailed list of aspects and determines it to be the authoritative definition of sources and methods, it could have many important consequences, not merely for future court cases but especially for educating collectors, producers, and users of intelligence as to their own security responsibilities. It could also become a basis for a single system of Foreign Intelligence Information in ways not now usefully provided by E. O. 11652.

25X1

11. I believe these three studies form a useful point of departure for the DCI and his deputies, and then for the USIB Principals. Obviously there are details which will require further study elsewhere within the security machinery, but if the problem is remanded to some committee or working group it could easily take ten years to coordinate a paper along least-common-denominator lines. Traditions die hard, and systems become their own excuse for being. I believe the total problem will require a unique combination of strong push from the top, throughout the Community, and of informed debates among the collectors and producers of sensitive information. Perhaps fairly short deadlines, with expressions of dissent rather than fully agreed positions (more or less as in national intelligence estimates) could allow the USIB Principals to recognize and resolve disagreements smoothly within a reasonable time. Full agreement and a perfect reform are probably both beyond human possibility, but inaction or piecemeal action can only go on weakening the security structure.